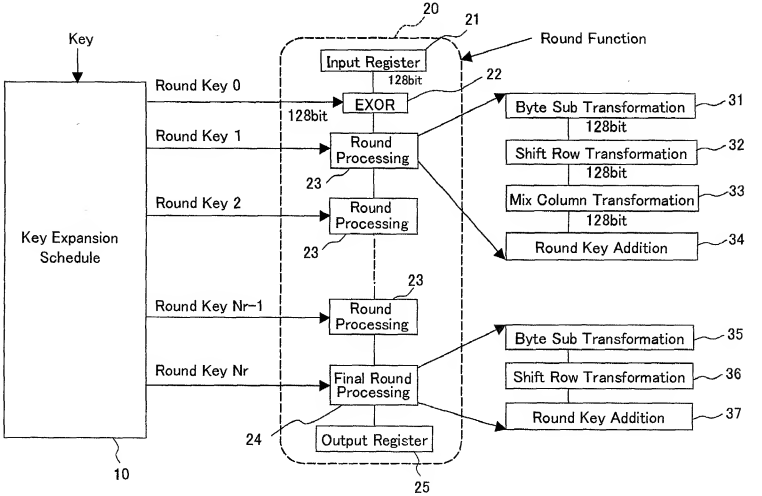


Fig. 1

```
Key Length = = 128bit or 192bit
KeyExpansion ( byte Key [ 4 * Nk]  word W [ Nb * ( Nr + 1 ) ]
{
        for ( i = 0 ; i < Nk ; i++ )
                W [ i ] = ( Key [ 4 * i ], Key [ 4 * i + 1], Key [ 4 * i + 3 ] );
        for ( i = Nk ; i < Nb * ( Nr + 1 ) ; i ++ )
        {
                temp = W [ i – 1 ];
                if ( i % Nk = = 0 )
                        temp = Sub Byte ( Rot Byte ( temp ) ) ^ Rcon [ i / Nk ];
                W [ i ] = W [ i – Nk ] ^ temp ;
        }
}


Key Length = = 256bit
KeyExpansion ( byte Key [ 4 * Nk]  word W [ Nb * ( Nr + 1 ) ]
{
        for ( i = 0 ; i < Nk ; i++ )
                W [ i ] = ( Key [ 4 * i ], Key [ 4 * i + 1], Key [ 4 * i + 3 ] );
        for ( i = Nk ; i < Nb * ( Nr + 1 ) ; i ++ )
        {
                temp = W [ i – 1 ];
                if ( i % Nk = = 0 )
                        temp = Sub Byte ( Rot Byte ( temp ) ) ^ Rcon [ i / Nk ];
                else if ( i % Nk = = 4 )
                        temp = Sub Byte ( temp );
                W [ i ] = W [ i – Nk ] ^ temp ;
        }
}
```

Fig. 2

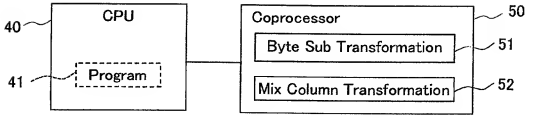

CPU
40
Program
41
Coprocessor
50
Byte Sub Transformation
51
Mix Column Transformation
52

Fig. 3

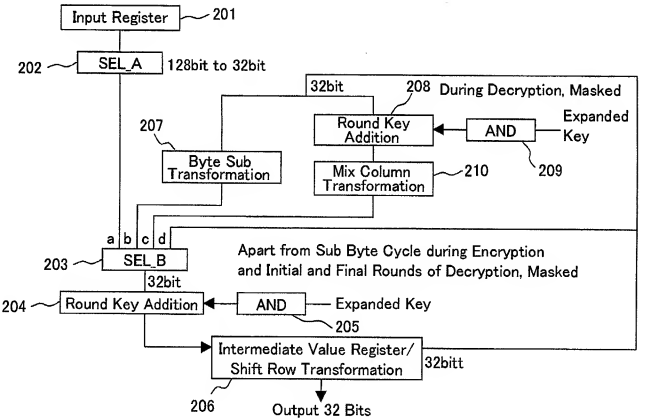
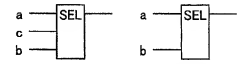


Fig. 4



Indicators for Selector Terminals

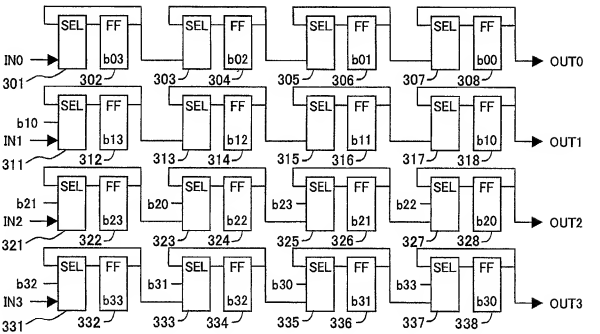


Fig. 5

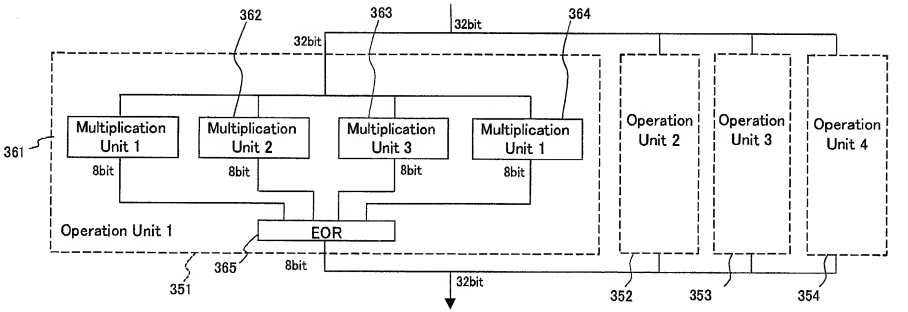

362
363
364
32bit
32bit
361
Multiplication Unit 1
Multiplication Unit 2
Multiplication Unit 3
Multiplication Unit 1
8bit
8bit
8bit
8bit
Operation Unit 1
EOR
365
8bit
351
32bit
Operation Unit 2
Operation Unit 3
Operation Unit 4
352
353
354

Fig. 6

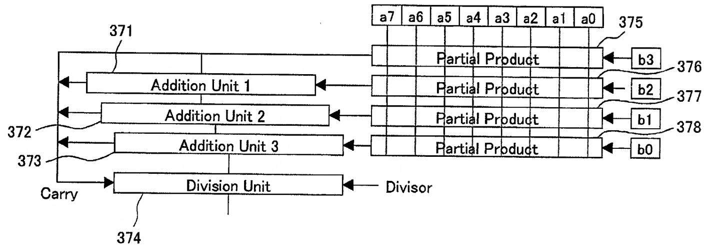

a7
a6
a5
a4
a3
a2
a1
a0
375
Partial Product
b3
376
Partial Product
b2
377
Partial Product
b1
378
Partial Product
b0
371
Addition Unit 1
372
Addition Unit 2
373
Addition Unit 3
Division Unit
Divisor
Carry
374

Fig. 7

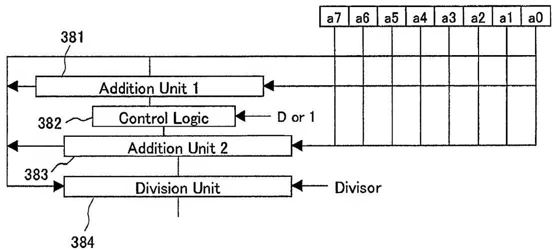

a7
a6
a5
a4
a3
a2
a1
a0
381
Addition Unit 1
382
Control Logic
D or 1
Addition Unit 2
383
Division Unit
Divisor
384

Fig. 8

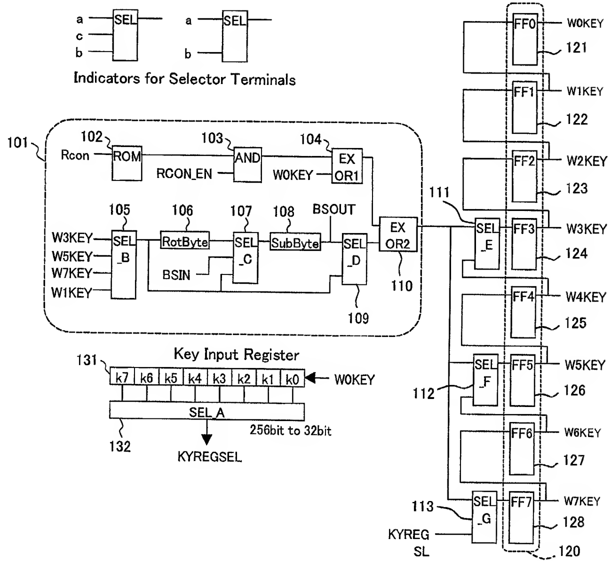

a
c
b
SEL
a
b
SEL
Indicators for Selector Terminals
101
102
Rcon
ROM
103
AND
RCON_EN
104
EX
OR1
W0KEY
105
106
107
108
BSOUT
W3KEY
W5KEY
W7KEY
W1KEY
SEL
_B
RotByte
SEL
_C
BSIN
SubByte
SEL
_D
EX
OR2
110
109
Key Input Register
131
k7
k6
k5
k4
k3
k2
k1
k0
W0KEY
SEL_A
256bit to 32bit
132
KYREGSEL
111
SEL
_E
112
SEL
_F
113
SEL
_G
KYREG
SL
FF0
W0KEY
121
FF1
W1KEY
122
FF2
W2KEY
123
FF3
W3KEY
124
FF4
W4KEY
125
FF5
W5KEY
126
FF6
W6KEY
127
FF7
W7KEY
128
120

Fig. 9

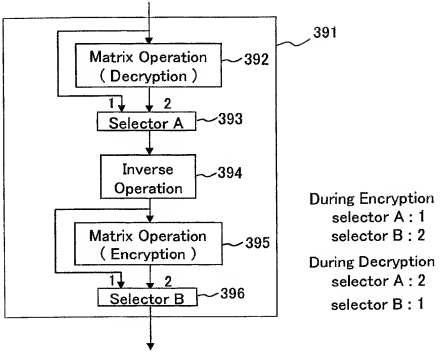

391
Matrix Operation
(Decryption)
392
1
2
Selector A
393
Inverse
Operation
394
Matrix Operation
(Encryption)
395
1
2
Selector B
396
During Encryption
selector A : 1
selector B : 2
During Decryption
selector A : 2
selector B : 1

Fig. 10

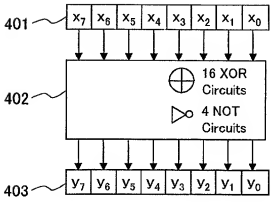

401
x_7 x_6 x_5 x_4 x_3 x_2 x_1 x_0
402
16 XOR Circuits
4 NOT Circuits
403
y_7 y_6 y_5 y_4 y_3 y_2 y_1 y_0

Fig. 11

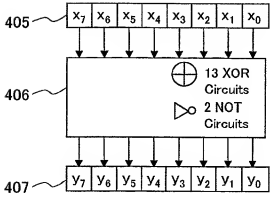

405
x_7 x_6 x_5 x_4 x_3 x_2 x_1 x_0
406
13 XOR Circuits
2 NOT Circuits
407
y_7 y_6 y_5 y_4 y_3 y_2 y_1 y_0

Fig. 12

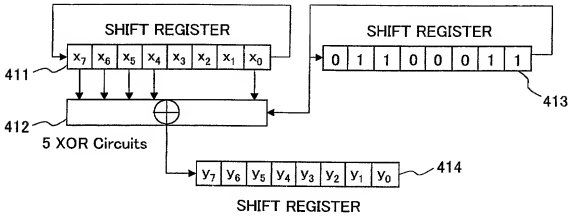

SHIFT REGISTER
SHIFT REGISTER
x_7 x_6 x_5 x_4 x_3 x_2 x_1 x_0
0 1 1 0 0 0 1 1
411
413
412
5 XOR Circuits
y_7 y_6 y_5 y_4 y_3 y_2 y_1 y_0
414
SHIFT REGISTER

Fig. 13

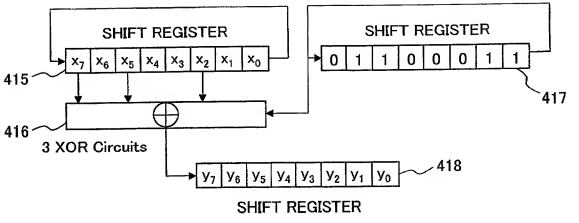

SHIFT REGISTER
SHIFT REGISTER
x_7 x_6 x_5 x_4 x_3 x_2 x_1 x_0
0 1 1 0 0 0 1 1
415
417
416
3 XOR Circuits
y_7 y_6 y_5 y_4 y_3 y_2 y_1 y_0
418
SHIFT REGISTER

Fig. 14